白皮書 • 2017 年 5 月

支付卡產業資料安全標準與 CA Privileged Access Management

目錄

簡介 3

第 1 節 3
PCI DSS 3.2 的主要要求

第 2 節 7
CA Privileged Access Manager 以及對 PCI DSS 3.2 要求的支援

第 3 節 19
結論

簡介

支付卡產業資料安全標準 (PCI DSS) 在 2004 年首度引進，以增進對信用卡持卡人資料的控管，並降低信用卡詐欺風險。每年必須進行認證，多年來皆定期推出新修訂版。最新的 3.2 版已於 2016 年 4 月開始實施。至 2018 年 1 月底，PCI DSS 與支付應用程式資料安全標準 (PA-DSS) 被認定為最佳實務作法，且自 2018 年 2 月 1 日起認定為要求。

第 1 節

PCI DSS 3.2 的主要要求

以下是 PCI DSS 的主要要求：

PCI 資料安全標準 – 高層級概觀

建立並維護安全的網路與系統	1. 安裝並維護防火牆配置，以保護持卡人資料 2. 勿針對系統密碼和其他安全性參數使用廠商提供的預設值
保護持卡人資料	3. 保護儲存的持卡人資料 4. 將在開放式公用網路上進行的持卡人資料傳輸加密
維護漏洞管理計畫	5. 保護所有系統對抗惡意軟體，定期更新防毒軟體或計畫 6. 開發並維護安全的系統與應用程式
實作強大的存取控制措施	7. 依據業務領域限制對持卡人資料的存取 8. 識別與驗證系統元件存取 9. 限制對持卡人資料的實體存取
定期監控並測試網路	10. 追蹤並監控所有對網路資源與持卡人資料進行的存取 11. 定期測試安全性系統與程序
維護資訊安全性原則	12. 維護可確保所有人員資訊安全性的相關原則

這些要求涉及範圍廣泛的高層級安全性措施。不過本文件要探討的是與管理特殊權限使用者相關的要求。

為什麼管理特殊權限存取如此重要？

如您所知，一條鎖鏈的強度取決於它最脆弱的一環。而通常，最脆弱的一環並非顯而易見。特殊權限身分往往是最不明顯的，直到發生違規或法務遵循失敗才會揭露出問題的存在。以下是特殊權限存取的幾個重要面向：

無所不在。任何組織中都有對於特定應用程式擁有較高存取權限的使用者。最常見的是具管理權限的使用者。然而，軟體開發的轉變與數位轉型，使得特殊存取權限的身分性質正在大幅改變。隨著組織轉向適用於基礎結構、平台和應用程式的虛擬環境及雲端，部門內的使用者取得了額外的權限。採用敏捷方法則產生更多應用程式對應用程式 (A2A) 的互動。還不只上述這些，因此可以想見，範圍只會變得更廣。

強而有力。顯然，對於應用程式或基礎結構的特殊存取權限會伴隨著重大的責任。這些使用者或身分擁有機密資料的存取權，任何惡意存取或意外事故均可能造成重大傷害並引發商譽危機。在上述每個案例中，如果使用者從任務關鍵性伺服器意外或有意地刪除資料，或者在生產伺服器上變更配置而未受監督，對業務會造成嚴重影響並引發關注。

首選目標。有鑑於特殊權限使用者及身分所擁有的存取權限之關鍵性，他們會受到圖謀不軌者的高度關注。通常他們會成為攻擊的目標，如果組織沒有正確維護安全性狀態，很可能就會受攻擊影響。

基於上述理由，管理特殊權限的使用者存取至關重要。此外，依據您的產業，這種存取也可能由法規直接或間接授權。PCI DSS 即擁有此授權。實際上，3.2 版納入的變更直接或間接地陳述了如何管理特殊權限存取。本文件的其餘部分將檢閱 PCI DSS 3.2 中對於特殊權限存取的特定要求。

特殊權限存取管理與 PCI DSS 3.2

3.2 版修訂了 PCI DSS 標準的數個章節，以反映不斷變化的業務現實面。其中部分變更是關於如何管理特殊權限存取。下表詳細說明了 PCI DSS 所定義的要求以及其與特殊權限存取管理的關聯。

要求	3.2 版的變更	對特殊權限存取管理的影響
要求 1： 安裝並維護防火牆配置，以保護持卡人資料。	已變更多個章節以示目的；刪除 1.3.3 一節。	此項要求規定，需管理可存取防火牆配置的使用者之群組及角色。此外，此要求隱含對特殊權限存取管理的要求： • 確保無輸出流量離開持卡人資料環境。 • 管理並監控配置檔案的所有變更。
要求 2： 勿針對系統密碼和其他安全性參數使用廠商提供的預設值。	此版本發佈的大多只是澄清說明。	本節對特殊權限身分及存取有廣泛的含義。現今多數軟體和硬體都有預設密碼。此外，這些密碼的相關原則差異很大。首先，需要識別標準之要求範圍下的所有資產。這些資產可能來自內部部署、虛擬或位於多個雲端環境中。特殊權限存取管理解決方案不僅應協助探索這些資產，且應協助為密碼設定原則、記錄工作階段，以及協助控制各邊界 (雲端、虛擬和內部部署) 對這些資產的存取。最後，受控存取需要夠細微，對這些系統中的安全性配置進行的任何變更都必須受到保護及監控。

要求 5： **保護所有系統對抗惡意軟體，定期更新防毒軟體或計畫。**	無變更。	有多種方法可對抗惡意軟體。儘管要求中明確提到了防毒軟體為最佳作法，組織應考慮所有方式來對抗惡意軟體。特殊權限存取管理提供了組織可對抗惡意軟體的方法。例如，對於具有防毒程式的系統，需充分控制升級與維護的管理存取。對於其他含有持卡人資料的系統，組織可以實施隔離策略、對應用程式及基礎結構進行分類，並控制對這些系統的存取。此外，可限制使用者執行的命令。還有，隨著機器學習和使用者行為分析的進步，我們可以主動減少任何可疑活動，即使是在帳戶接管的情況下。若考慮到組織所面臨的挑戰之規模和範圍，這點更為關鍵，也使手動技術難以實行。最後，特殊權限存取管理解決方案還能使用鍵盤記錄和螢幕錄製等技術來監控和記錄任何活動。
要求 6： **開發並維護安全的系統與應用程式。**	變更僅限於特定章節，且用於提供指導。	本節探討在開發及維護存取持卡人資料的軟體和系統時要遵循的整體安全性最佳作法。對於此項要求的指導涵蓋以下層面： • 確保最新的修補程式套用於系統 • 開發遵循適當安全性程序的軟體 • 遵循生產和非生產應用程式及伺服器之間的分工 特殊權限存取管理解決方案可大幅協助處理這項要求。例如，在維護系統和套用修補程式等等時，組織需確保有充分的控制程序，並配合適當的驗證及監督層級。比方說，儘管已允許系統管理使用者執行命令來修補伺服器，但若為生產系統，則需強制執行其他控制和核准。應用程式可能可藉程式化方式存取持卡人資料，其需要認證來執行此項操作。最後，此項要求規定，對於存取不同環境 (開發人員、測試和生產環境) 的使用者必須進行職務分工。特殊權限存取管理解決方案可協助管理這些認證，而非將其內嵌到應用程式中。特殊權限存取管理解決方案與自動化工具之間的整合可達成職務分工的要求。

要求 7： **依據業務領域限制對持卡人資料的存取。**	對指導和測試進行變更，以涵蓋多個系統。	此項要求規定，對於包含機密資料的任何應用程式或系統，不同使用者的存取必須根據角色、業務需求和最低權限進行控制。此種存取應進行記錄且可稽核。 特殊權限存取管理解決方案有助於處理這項要求，透過管理群組中的使用者，並定義在特定應用程式或一組應用程式上允許使用者執行哪些項目。此外，利用與其他解決方案的整合，特殊權限存取管理解決方案可針對各種應用程式和系統的存取，提供以工作流程為基礎的佈建和取消佈建。最後，此種存取也可以進行錄製、記錄和稽核。
要求 8： **識別與驗證系統元件存取。**	也許目前版本中最重大的變更就在於此項要求。現在對於機密資料的所有非以 Web 為基礎的存取以及遠端存取都需要透過多元驗證 (MFA) 進行保護。此外，早期要求的雙重要素驗證已擴展為多元驗證。	此項要求對特殊權限帳戶具有深遠影響。所有特殊權限帳戶，無論是直接存取或間接存取以及遠端存取，皆需透過 MFA 提供保護。所有使用者存取都必須進行記錄且可以追蹤。此項要求規定，所有存取系統的使用者均需具有唯一身分。使用者的存取必須根據最低權限進行配置，且所有動作都必須可以稽核。必須實施適當的使用者生命週期管理 (佈建、取消佈建和修改)，以提供使用者及其存取權限的建立、刪除及修改。包括認證在內的任何使用者資訊都必須使用強式密碼編譯來管理。任何密碼或複雜密碼都應遵守對於強度和輪換的特定原則。此項要求也規定，共用認證不應用於特定應用程式。適當控制為必要，在含有持卡人資料的資料庫上執行的命令會根據角色和業務需求 (僅資料庫管理員) 而受限，且拒絕所有其他存取。
要求 10： **追蹤並監控所有對網路資源與持卡人資料進行的存取。**	新增一項額外要求，需要在服務提供者環境中進行即時偵測以及任何安全性失效的報告。	此項要求規定，需維護所有使用者的完整稽核追蹤、其存取權限以及網路上所有資源中任何規則、配置和對特定欄位的存取控制中可能發生的任何變更。

要求 11： **定期測試安全性系統與程序。**	此處多數的變更都與滲透測試要求有關，該要求並不會直接影響特殊權限存取管理。	此項要求的其中一項任務是，必須實施入侵偵測系統來判定風險。然而，隨著運算環境的變化，現在可以使用機器學習技術，根據使用者行為來主動降低威脅。
要求 12： **維護可確保所有人員資訊安全性的相關原則。**	最新版本中對此項要求的變更主要在於澄清說明和測試程序。	任何特殊權限存取管理解決方案應支援管理存取的原則，並允許特殊權限使用者為所有人員建立、修改和刪除安全性原則。所有動作都應該可以稽核，且可追蹤進行該交易的特定使用者。

第 2 節

CA Privileged Access Manager 以及對 PCI DSS 3.2 要求的支援

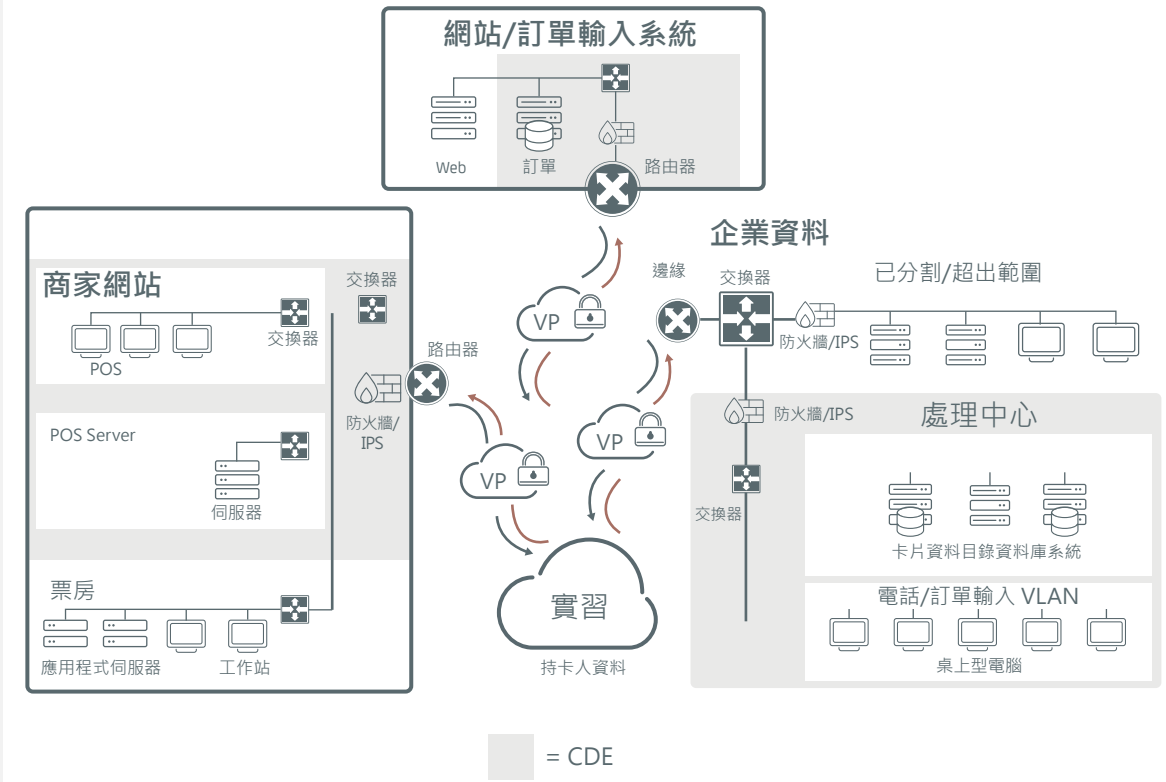
中斷網際攻擊狙殺鍊

狙殺鍊的基本概念是攻擊者會採取一個重複的模式存取系統 (或延伸存取)，再提升權限。這些權限接著被用來水平或垂直移動並存取另一個系統或延伸現有的存取權，或一再提升權限並進行連鎖破壞行為，直到達成最後目的為止。若在循環中的任何時間點能夠打破這個連鎖行為，就能夠制止攻擊行動達成目的。

CA Privileged Access Manager (CA PAM) 提供能夠協助中斷網際攻擊狙殺鍊的功能。例如，CA PAM 支援特權帳戶多元驗證，使攻擊變得更為困難，因為攻擊者必須破解單一帳戶的多重憑證。此外，每個特權帳戶只有最低的權限可對每個持卡人資料環境 (CDE) 發出命令，減少對機密資訊的存取權，如此一來攻擊者要對有興趣的資料取得未授權的存取就變得更為困難。

CA PAM 協助打破網際攻擊狙殺鍊的另一個方式是透過支援網路分割。這個方法可以限制特定特權帳戶可以存取的子網路，以及每個子網路可管理的系統。網路分割有助於限制攻擊不至橫向蔓延到其他系統，也限制攻擊者對於組織網路的能見度。此外，CA PAM 提供封包過濾代理程式 (SFA)，防止管理員對另一個系統開啟未授權的網路連線，例如嘗試進行 SSH 連線或以 Telnet 連線到未獲 CA PAM 原則授權的主機。

圖 1.
PCI DSS 合規分解圖。



CA 的特殊權限存取管理解決方案可協助組織處理 PCI DSS 3.2 的要求。本節會說明解決方案的各種功能。此外，若與其他整合的 CA 安全性解決方案結合時，組織可採用強大、可擴展且全功能的解決方案來滿足其 PCI DSS 之需求。下表更詳細地討論了 CA PAM 如何協助處理最新的 PCI DSS 要求。

要求	3.2 版的變更
1.1：建立並實施防火牆和路由器配置標準。	CA 的特殊權限存取管理解決方案，可限定僅供特定組合的特殊權限使用者來建立、實施和管理防火牆和路由器配置。
1.1.5：網路元件管理的群組、角色和責任說明。	CA 的解決方案可建立使用者群組，為這些使用者指派特定角色和權限，以便對於網路元件、伺服器和應用程式管理的適當責任進行職務分工。CA 也支援虛擬網路環境管理，例如 VMWare NSX，提供全方位且可擴展的解決方案。若與 CA 身分識別管理與支配解決方案整合時，將使用者指派到群組和角色的流程可以自動化。

1.2.1：將輸入和輸出流量限制在持卡人資料環境所需的流量以內，並明確拒絕所有其他流量。	儘管此項要求側重於監控輸入和輸出流量，但有了 CA Privileged Access Manager Server Control，組織可規定在一組伺服器上不允許執行特定命令，進而確保資料不會離開組織的網路。
2：勿針對系統密碼和其他安全性參數使用廠商提供的預設值。	CA PAM 支援變更預設密碼和其他安全性參數，例如已允許的管理員網路存取方法。
2.1：在網路上安裝系統之前，務必變更廠商提供的預設值，並移除或停用不必要的預設帳戶。	CA PAM 可保存並管理系統管理的密碼/認證。這包括強制變更預設密碼。
2.3：使用強式密碼編譯為所有非主控台管理存取進行加密。針對以 Web 為基礎的管理和其他非主控台管理存取使用 SSH、VPN 或 SSL/TLS 等技術。	CA PAM 強制執行存取原則，規定個人只能透過核准的 (加密) 通訊協定來存取系統。由於所有管理密碼和認證都保存在加密的保存庫中，因此管理員無法規避這些存取原則。CA PAM 提供 SSL VPN 來保護管理流量免受竊聽和操縱，且對 CA PAM 主控台本身的存取也受到 TLS (HTTPS) 的保護。
5.1：在所有常受惡意軟體影響的系統 (特別是個人電腦和伺服器) 上部署防毒軟體。	CA 特殊權限存取管理允許特定使用者在一組系統上管理特定應用程式的安裝與升級。這可用系統管理使用者的群組或角色作為基礎。系統和伺服器也可列入白名單或黑名單，以協助確保任何惡意軟體無法進行傳播。使用 CA Threat Analytics for PAM，組織還可偵測可疑活動並啟動風險減緩策略。
6：開發並維護安全的系統與應用程式。	CA PAM 協助組織從持卡人資料處理系統中的指令碼、程式碼和配置檔案中去除 A2A 密碼，消除了管理密碼以純文字形式儲存的重大漏洞，避免其由應用程式開發人員和測試人員存取。雖然在要求中沒有特別提及此漏洞，但它仍是個極高風險的問題，特別是與持卡人資料庫整合的本地系統、應用程式和指令碼 (例如針對報告和上游或下游交易之目的)。

6.3：安全地開發內部和外部軟體應用程式 (包括以 Web 為基礎的應用程式管理存取)，具體如下： • 符合 PCI DSS (例如安全驗證和記錄)。 • 依據業界標準和/或最佳作法。 整合軟體開發生命週期中的資訊安全性。	參閱要求 6.3.1。
6.3.1：在應用程式啟用或發行給客戶之前，移除開發、測試和/或自訂應用程式帳戶、使用者 ID 和密碼。	利用 CA PAM，組織可將密碼從應用程式代碼移動到加密的保存庫，並使用 CA PAM API 以規定僅特定授權的呼叫應用程式可以要求密碼。密碼從保存庫到目標系統 (跨網路和記憶體) 均維持加密狀態。此外，透過與 CA 身分識別管理與支配解決方案的整合，只有針對管理應用程式帳戶、使用者和認證之佈建和取消佈建取得允許的使用者才能執行此操作。
6.4：針對系統元件的所有變更，遵循變更控制流程及程序。流程必須包含以下：	參閱要求 6.3.1。
6.4.2：開發/測試與生產環境之間的職務分工。	CA PAM 針對用於開發、測試和生產的系統上之特殊權限帳戶強制執行以角色為基礎的存取控制。若與 CA 身分識別管理與支配解決方案整合時，CA PAM 可根據角色、特殊權限和職務分工原則來提供適當的使用者存取等級。
7：依據業務領域限制對持卡人資料的存取。	CA PAM 實施一套全面的控制項，用於限制對系統元件和持卡人資料的存取。這些控制項可協助組織實施零信任模型，將最低權限的概念擴展為「沒有特定授權就沒有特殊權限」。零信任模型會強制執行細部存取控制，對所有特殊權限使用者的工作階段進行監控和記錄。透過特殊權限支配 (CA PAM 和 CA 身分識別管理與支配解決方案間的整合) 即可規定，針對所有系統的建立、讀取、更新和刪除操作之整個使用者生命週期皆需受到控制。這可提供職務分工並簡化合規報告。

7.1：限制對系統元件和持卡人資料的存取權限，僅開放給工作上需要存取的人員。	CA PAM 在各個層面實施最低權限原則。它對特殊權限使用者強制執行細部存取控制，必須明確取得授權以存取伺服器、網路裝置和其他系統元件。解決方案也使用命令過濾 (白名單和黑名單) 來限制授權使用者可以執行的命令。有了特殊權限支配 (CA PAM 和 CA 身分識別管理與支配解決方案)，使用者可以透過完整的核准流程取得對這些資料的存取權限，任何特殊權限的變更均可管理，且所有特殊存取權限都可以針對法規要求來進行報告和認證。
7.1.1：定義每個角色的存取需求，包括： • 每個角色因職責所需存取的系統元件和資料資源。 • 存取資源所需的權限等級 (例如使用者、管理員等)。	由於 CA PAM 完全支援以角色為基礎的存取控制，它提供一套適於定義每個管理角色 (例如資料庫、網路或系統管理員) 存取需求的機制。這包括限制每個管理角色可存取該系統元件中的哪些系統元件和資料資源。
7.1.2：將特殊權限使用者 ID 的存取權限，限制為執行工作職責所需的最低權限。	這是 CA PAM 功能的核心。每個特殊權限使用者 ID 或特殊權限使用者 ID 群組的存取權限僅限於每個授權系統元件所需的命令。
7.1.3：根據人員的工作類別和職責指定存取權限。	CA PAM 會強制執行適用於個人或群組的原則。可在 CA PAM 中直接或運用解決方案的整合來建立群組和角色定義，以及使用已經存在於企業目錄中的群組和角色定義。此外，透過與 CA 身分識別管理與支配解決方案的整合，根據業務角色、群組或位置對使用者佈建與取消佈建存取權限的流程，使得流程更容易管理。對系統管理使用者授予的錯誤權限可以進行補救。
7.1.4：需要授權方的書面核准，其中會指定所需權限。	CA PAM 可以在發行密碼之前強制執行需要 (且會記錄) 授權人員核准的雙重授權。
7.2：建立系統元件的存取控制系統，該系統會根據使用者領域來限制存取，且除非特別允許，否則系統會設為「全部拒絕」。此存取控制系統必須包含以下：	CA PAM 將驗證與授權分離。使用者使用強式 (多重要素) 驗證方式登入 CA PAM。登入後，使用者會取得已明確授權存取的元件清單。使用者無法看見或存取未授權的元件。
7.2.1：涵蓋所有系統元件。	如 PCI DSS 所定義，系統元件包含伺服器、網路裝置和應用程式。CA PAM 涵蓋所有 PCI DSS 定義的元件，包括現成的應用程式。

7.2.2：根據工作類別和職責將特殊權限指派給個人。	CA PAM 拒絕所有存取，除非透過個人或群組原則明確授予個人存取權限。
7.2.3：預設「全部拒絕」設定。	CA PAM 拒絕所有存取，除非透過個人或群組原則明確授予個人存取權限。
8：識別與驗證系統元件存取。	CA PAM 需要唯一使用者登入來識別每個使用者，且該解決方案支援許多驗證技術。確保對共用帳戶的任何存取都可追溯到實際使用者，這點也非常重要。在任何自動化存取系統元件的情況下，需要知道哪個使用者的動作啟動了存取。CA PAM 為這種存取提供了解決方案。為了將系統元件存取的風險降到最低，CA Threat Analytics for PAM 提供了標記存取的方法，以進一步減緩風險。
8.1：定義並實施原則與程序，以確保對所有系統元件上的非消費者使用者和管理員進行適當的使用者識別管理，具體如下：	CA PAM 支援強制執行原則，其用於管理所有系統元件的特殊權限帳戶之身分識別。詳細資訊請參閱以下 8.1.1 至 8.1.8。
8.1.1：在允許存取系統元件或持卡人資料之前，為所有使用者指定唯一的 ID	CA PAM 需要唯一使用者登入至 CA PAM 平台，然後對授權的系統元件建立特殊權限工作階段。在此配置中，組織可針對基礎結構元件 (例如 root) 來運用「共用帳戶」以便管理，同時還可從每個特殊權限工作階段追蹤到特定的個人 (不只是 IP 位址)。
8.1.2：控制使用者 ID、認證和其他識別項物件的新增、刪除和修改。	CA PAM 會強制執行職務分工，因此只有特定授權的管理使用者可以變更其特殊權限 ID 和其他認證。這些特殊的 CA PAM 管理使用者必須使用強式多重要素驗證方法，且每個工作階段均會進行記錄。透過與 CA 身分識別管理與支配解決方案的整合，可以進一步增強這點。
8.1.3：立即撤銷任何已終止的使用者之存取權限。	CA PAM 讓組織能夠立即終止特殊權限已結束的使用者對所有系統元件的存取。
8.1.4：至少每 90 天移除/停用非作用中的使用者帳戶。	CA PAM 支援自動停用一段時間未使用的 CA PAM 帳戶。

8.1.5：透過遠端存取管理廠商用來存取、支援或維護系統元件的 ID，具體如下： 僅在需要的時段內啟用，不使用時就停用。 使用時會受監控。	CA PAM 對於管理特殊權限廠商 ID 與管理任何其他特殊權限 ID，其功能相同。這包括對廠商執行限時存取。此外，解決方案會監控及記錄每個特殊權限工作階段，且可傳送警示，並在出現違反原則的嘗試時自動終止存取。
8.1.6：在六次以下嘗試失敗後鎖定使用者 ID，以限制重複存取嘗試。	CA PAM 強制執行嘗試失敗原則，包括經管理員定義的存取嘗試失敗次數後鎖定 CA PAM 帳戶。
8.1.7：將鎖定的持續時間設為最少 30 分鐘，或者直到管理員啟用使用者 ID。	CA PAM 可以強制執行選項，例如鎖定帳戶直到授權管理員重新啟用它。
8.1.8：如果工作階段閒置超過 15 分鐘，使用者需要重新驗證以重新啟動終端或工作階段。	CA PAM 可以設定工作階段逾時，預設為 10 分鐘。
8.2：除了指定唯一的 ID，若要確保對所有系統元件上的非消費者使用者和管理員進行適當的使用者驗證管理，至少須採用以下其中一種方法來驗證所有的使用者：您記得的東西，例如密碼或複雜密碼。 您擁有的東西，例如權杖裝置或智慧卡。 您身上的一部份，例如生物特徵辨識。	CA PAM 支援與多種驗證方法的整合，包括強式、多重要素驗證系統。解決方案會將驗證要求傳遞到所選的驗證系統 (如 AD、RADIUS、智慧卡)。個人一旦成功通過驗證，CA PAM 將根據 CA PAM 中的個人或群組原則，提供使用者可存取的明確授權資源清單，以及可使用的存取方法。這使組織能夠將驗證與授權分離。
8.2.1：使用強式密碼編譯，可讓所有驗證認證 (如密碼/複雜密碼) 在所有系統元件上的傳輸和儲存過程中都無法讀取。	CA PAM 將密碼和其他驗證認證儲存在加密的保存庫中。解決方案使用 FIPS 140-2 安全性核心進行所有加密操作。與硬體安全模組 (HSM) 的整合可達成更高等級的 FIPS 140-2 合規性。密碼和其他認證會透過安全/加密通道來傳輸。
8.2.2：驗證使用者身分識別後，才能修改驗證認證，例如執行密碼重設、佈建新權杖或產生新的金鑰。	CA PAM 可進行設定，要求先成功進行驗證後，才能啟用密碼重設、產生新的加密金鑰等等。
8.2.3：密碼/複雜密碼必須符合以下條件： 最小長度須至少七個字元。 同時包含英數字元。 或者，密碼/複雜密碼必須至少具有等同於上述指定參數的複雜性和強度。	CA PAM 執行業界標準的密碼長度和強度/組合原則，包括最小密碼長度和不同類型字元的使用。

8.2.4：至少每 90 天變更一次使用者密碼/複雜密碼。	CA Privileged Access Manager 會在時間間隔內強制變更密碼。系統的密碼管理功能會根據系統中建立的原則自動執行變更。
8.2.5：不允許個人提交的新密碼/複雜密碼與最近四次所用過的密碼/複雜密碼相同。	CA PAM 執行業界標準之完全可設定的密碼重複使用原則，其中包含由管理員決定的設定，在重複使用一組密碼之前需要輪替多少次其他密碼，以及在變更一組密碼之前必須使用該密碼多少天。
8.2.6：將首次使用的密碼/複雜密碼針對每個使用者設定為唯一值，並在第一次使用後立即變更。	CA PAM 實施一套全面的密碼原則，包括密碼組合、重複使用和過時。這些原則支援一次性使用，甚至可以設定在每次使用後自動設定新密碼。 另一個選擇是允許密碼簽選，並自動設定此密碼可行的短期時限。
8.3：使用多重要素驗證來保護所有個人的非主控台管理存取以及所有對 CDE 的遠端存取。	CA Privileged Access Manager 支援各種多元驗證方法，且支援 RADIUS 與 X.509 憑證以及智慧卡。在啟用特殊權限使用者對授權資源的存取之前，CA Privileged Access Manager 可以強制執行強式多元驗證。此外，若與 CA 領先業界的進階驗證功能整合，組織即可啟動多元驗證。有了 Threat Analytics of PAM，特殊權限使用者的行為違反正常時，就可以終止該工作階段。下次登入時可以強制進行多元驗證。
8.3.1：納入遠端網路存取的多元驗證，該存取源自網路外部的人員 (包括使用者和管理員) 和所有第三方 (包括廠商為支援或維護所進行的存取)。	CA PAM 支援各種多元驗證方法，且支援 RADIUS 與 X.509 憑證以及智慧卡。在啟用特殊權限使用者對授權資源的存取之前，CA PAM 可以強制執行強式多元驗證。此外，若與 CA 領先業界的進階驗證功能整合，組織即可啟動多元驗證。有了 CA Threat Analytics for PAM，特殊權限使用者的行為違反正常時，就可以終止該工作階段。下次登入時可以強制進行多元驗證。

8.5：勿使用群組、共用或通用 ID、密碼或其他驗證方法，如下： • 通用使用者 ID 遭停用或移除。 • 共用使用者 ID 不存在系統中。管理和其他關鍵功能。 • 共用和通用使用者 ID 不用於管理任何系統元件。	在傳統配置中，共用帳戶的問題來自於無法分辨是誰引發了問題。如果每個使用者都以 root 或管理員身分登入，則每個特殊權限使用者都會是匿名的。但共用、通用或群組帳戶大幅簡化系統元件的配置和管理，尤其是在大型網路中。有了 CA PAM，您可以同時擁有兩個世界中的最佳功能——具有完全責任歸屬 (且可驗證) 的共用帳戶。組織可以繼續使用共用帳戶來設定伺服器、網路裝置和其他元件，但仍擁有特定且可驗證的記錄，確切指出登入共用帳戶的是哪個使用者以及其所執行的操作。這些共用帳戶的密碼儲存在 CA PAM 保存庫中，因此使用者被迫需登入 CA PAM，以取得共用帳戶的存取權限。一旦使用者登入共用帳戶，CA PAM 會監控並記錄所有內容，因此使用共用帳戶所執行的任何特殊權限使用者活動，都可以追溯到特定的使用者。
8.6：使用其他驗證機制 (例如實體或邏輯安全性權杖、智慧卡、憑證等) 時，這些機制的使用必須進行指派如下： 驗證機制必須指派給個人帳戶，且不能在多個帳戶之間共用。 實體和/或邏輯控制必須就位，以確保只有預定帳戶可以使用該機制取得存取權限。	CA PAM 支援多種驗證機制的使用，包括安全性權杖、智慧卡和數位憑證。這些機制每項都可以指派給個人唯一 ID，並連帶使用其他驗證機制以協助確保只有獲得授權的人可透過安全性權杖、智慧卡或數位憑證進行存取。
8.7：對含有持卡人資料的任何資料庫之存取 (包括由應用程式、管理員和所有其他使用者的存取) 受限制如下： 對資料庫的所有使用者存取、使用者查詢和使用者動作都是透過編程方法。 只有資料庫管理員才能直接存取或查詢資料庫。 資料庫應用程式的應用程式 ID 只能由應用程式 (非個人使用者或其他非應用程式流程) 使用。	CA PAM 僅限授權管理員可以直接存取持卡人資料庫。解決方案中也規定，應用程式帳戶只能由應用程式使用。
10.1：實施稽核追蹤，將系統元件的所有存取連結至每個個別使用者。	CA PAM 會將所有特殊權限存取連結到特定的使用者。它支援強式多元驗證，以協助確保只有獲得授權的個人能夠使用特殊權限帳戶存取系統元件，因此每個特殊權限工作階段都可以歸屬到特定的授權使用者。
10.2：實施所有系統元件的自動化稽核追蹤，以重建以下事件：	特殊權限使用者在系統元件 (伺服器、資料庫、網路裝置、應用程式等) 上執行的每個動作都由 CA PAM 記錄在防篡改記錄檔中，只有特定授權的使用者可以存取和檢閱。詳細資訊請參閱以下 10.2.1 至 10.2.7。

10.2.1：對持卡人資料的所有個人使用者存取。	對持卡人資料庫的所有管理員存取 (例如由授權的資料庫管理員) 都由CA PAM 進行監控和記錄。
10.2.2：由任何具有 root 或管理權限的個人所執行的所有動作。	CA PAM 會監控和記錄所有特殊權限活動。即使組織使用的是共用管理帳戶，CA PAM 也可以將所執行的每個動作歸屬到特定的唯一使用者。
10.2.3：所有稽核追蹤的存取。	CA PAM 提供職務分工，因此只有特定授權的使用者可以檢閱 CA PAM 記錄檔和錄製。每當授權使用者檢閱記錄檔時，檢閱一事也會記錄下來，且可以進行錄製。
10.2.4：無效的邏輯存取嘗試。	CA PAM 會追蹤源自 CA PAM 平台的所有無效邏輯存取嘗試。首先，只有授權的使用者可以存取 CA PAM，且授權的使用者只會取得已明確授權的系統之存取權限。存取授權系統之後，CA PAM 也會防止嘗試使用已授權系統來存取未授權系統 (蛙跳或 RDP 跳接)。CA PAM 不會記錄在平台外所執行的失敗登入嘗試，例如嘗試直接連線並登入伺服器。但由於所有密碼/認證都儲存在 CA PAM 保存庫中，使用者無法得知密碼，因此只能透過 CA PAM 平台登入這些系統。
10.2.5：身分識別和驗證的使用及變更機制 (包括但不限於建立新帳戶和提高權限) 以及對於具有 root 或管理權限的帳戶之所有變更、新增或刪除。	CA PAM 會記錄特殊權限帳戶的所有身分識別和驗證活動，包括涉及這些帳戶的所有變更以及這些帳戶的使用情況。
10.2.6：稽核記錄檔的初始化、停止或暫停。	CA PAM 沒有記錄檔條目來顯示記錄已初始化；而是在預設下，解決方案會不斷產生記錄檔。
10.2.7：系統層級物件的建立和刪除。	在 CA Privileged Access Manager 中，授權管理員可以建立和刪除目標伺服器、帳戶、密碼、群組、使用者等等。
10.3：針對所有系統元件的每個事件，記錄至少以下稽核追蹤條目：	CA PAM 會針對所有系統元件的特殊權限存取記錄完整的稽核追蹤。詳細資訊請參閱以下 10.3.1 至 10.3.6 的回應。

10.3.1：使用者身分識別。	使用者透過強式多元方法進行驗證，因此唯一使用者會被擷取在 CA PAM 所維護的記錄檔和錄製中。
10.3.2：事件類型。	CA PAM 將 Syslog 事件分類，包括登入/登出嘗試、違反原則嘗試、遠端工作階段建立等。
10.3.3：日期和時間。	日期和時間被擷取為 Syslog 和工作階段記錄串流的一部分。
10.3.4：成功或失敗指示。	對於與成功或失敗有關的每個事件，例如登入/登出嘗試，CA PAM 會記錄該事件為成功或失敗。
10.3.5：事件起源。	CA PAM 會擷取每個事件中用來存取解決方案的唯一使用者身分識別和來源 IP 位址。
10.3.6：受影響的資料、系統元件或資源的身分識別或名稱。	對於影響系統元件、資源等的事件，受影響的目標 (如主機名稱) 和存取系統的使用者之身分識別會被擷取。
10.4：使用時間同步化技術，同步所有關鍵的系統時鐘與時間，並確保實施以下項目以便取得、分配及儲存時間。	CA PAM 支援業界標準的時間同步化技術 - 網路時間協定 (NTP)。
10.4.1：關鍵系統具有正確且一致的時間。	CA PAM 使用 NTP 執行時間同步化，以確保其稽核記錄檔和錄製具有正確且一致的時間戳記。
10.4.2：時間資料受到保護。	CA PAM 可設定使用已驗證的 NTP，其可提供比基本 NTP 更高層級的完整性。
10.4.3：時間設定是取得自業界公認的時間來源。	已指定兩個預設的時間伺服器，授權的 CA PAM 管理員可以增強和/或變更這些伺服器。
10.5：保護稽核追蹤，使其無法被更改。	CA PAM 記錄檔和錄製均受到保護，免於遭受未經授權的存取和修改，且若發生任何變更都會進行偵測。
10.5.1：僅限相關工作需求者可檢視稽核追蹤。	CA PAM 記錄檔和錄製只能由明確授權的人員存取，遵循最低權限和以角色為基礎的存取控制原則。

10.5.2：保護稽核追蹤檔案免受未經授權的修改。	所有 CA PAM 記錄檔和錄製均使用加密雜湊技術以防竄改。若檔案被篡改，CA PAM 會發出通知。
10.5.3：將稽核追蹤檔案迅速備份到難以更改的集中式記錄伺服器或媒體。	CA PAM 提供 Syslog 轉送，其允許將所有 CA PAM 記錄檔備份到集中式 Syslog 伺服器、一次性寫入媒體和其他形式的記錄儲存體及封存。
10.5.5：在記錄檔上使用檔案完整性監控或變更偵測軟體，以確保現有的記錄資料發生變更時會產生警示 (新增新資料則不會引發警示)。	CA PAM 記錄檔和錄製均使用加密雜湊技術以防竄改。除了新資料的標準新增之外，對現有記錄檔或錄製的任何修改都會進行偵測。
10.6 (包括 10.6.1 至 10.6.3)：檢閱所有系統元件的記錄檔和安全性事件，以識別異常或可疑活動。	CA Threat Analytics for PAM 提供一個強大且以機器學習為基礎的使用者行為分析 (UBA) 解決方案。此解決方案可與 SIEM 解決方案及其他企業記錄解決方案搭配使用，可用於判定以使用者為基礎的活動之相關風險。判定出的任何風險都可使用各種技術來緩解。
10.7：稽核追蹤歷程記錄保留至少一年，且最少三個月的記錄可立即用於分析 (例如線上、封存或可從備份還原)。	由於 CA PAM 使用 Syslog，因此如有必要可在 Syslog 伺服器上長期保留稽核追蹤。這可釋放本機 CA PAM 系統上的儲存空間，同時讓記錄資料可立即用於分析。本機 CA PAM 系統可保留記錄檔長達四個月。
12：維護可確保所有人員資訊安全性的相關原則。	CA PAM 讓組織能夠擷取和執行保護持卡人資料的特殊權限使用者原則。此解決方案可輕鬆證實，對於涉及持卡人資料處理的每個系統元件所需的控制皆已就位。
12.2：實施風險評估流程： 該流程每年至少執行一次，並在環境發生重大變更 (例如收購、合併、搬遷等) 時立即執行。 該流程可識別關鍵資產、威脅和漏洞，並 產生正式的風險評估。	CA PAM 讓組織能夠檢閱記錄檔和錄製 (使用類似 DVR 的播放)。由於所有違反原則的嘗試都會記錄下來，CA PAM 讓組織能夠將檢閱工作集中在發生違反原則嘗試的管理工作階段中，然後快速檢查其他工作階段有無異常之處。

第 3 節

結論

由於 PCI DSS 3.2 版的規定將自 2018 年 2 月起成為強制要求，因此組織必須考慮可調整的解決方案，以協助解決未來法務遵循的問題。為了實現這些目標，需考慮以下因素：

- **可調整性和高可用性。**有鑑於在 PCI DSS 適用範圍內的系統和應用程式皆含有機密的持卡人資料，不只這些應用程式應具有高可用性，保護應用程式的解決方案也應如此。因此，任何特殊權限存取管理解決方案都應具有高度的可調整性，不只是為了提供對使用者及其存取的驗證和授權，也是為了工作階段管理和記錄。
- **可擴充。**隨著越來越多系統和應用程式進入 PCI DSS 範圍內 (根據其業務增長或部署階段)，任何特殊權限存取管理解決方案都應該易於擴充，以便迅速有效地納入新的基礎結構和應用程式。此外，隨著使用者、系統和應用程式的數量迅速增加，手動監控使用者活動變得十分困難。任何特殊權限存取解決方案都需要提供以分析為基礎的風險緩解策略。特殊權限存取管理很可能需要與其他解決方案整合，為該標準提供全方位的支援，這是個重要的考慮因素。
- **擁有成本。**隨著特殊權限存取管理解決方案所需的功能增加，一段時期 (通常 3–5 年) 的擁有成本不應該太高。例如，特殊權限存取管理解決方案一開始可能只是簡單的密碼保存，但 PCI DSS 要求的更多，包括密碼原則、授權和工作階段管理和記錄等功能。如果這些功能都各別提供，組織可能需要在不同階段考慮基礎結構、技能和授權以及部署成本的需求。此外，每個階段的維護和整合成本可能有所不同，因此雖初期階段的入門價格較低，但在未來階段卻是不可行的。

若要深入了解 CA 特殊權限存取管理解決方案如何使組織受益，請造訪 **ca.com/pam**

與 CA Technologies 聯繫

CA Technologies (NASDAQ: CA) 創造的軟體能為公司轉型注入源源不絕的能量，使他們得以掌握應用經濟的良機。軟體是從事各產業之公司的核心。從計畫到開發、管理及安全性，CA 與來自全球的公司通力合作，跨越行動、私有與公有雲端、分散式與大型機環境等限制，一同改變我們生活、交易及溝通的方式。
詳情請造訪 ca.com/tw。

CS200-298517_0817